Electronic Footprints in the Sand

Technologies for Assisting Domestic Violence Survivors

Martin Emms, Budi Arief, and Aad van Moorsel

School of Computing Science, Newcastle University, Newcastle upon Tyne NE1 7RU, UK
{martin.emms,budi.arief,aad.vanmoorsel}@newcastle.ac.uk

Abstract. With the rapid growth and spread of Internet-based social support systems, the impact that these systems can make to society – be it good or bad – has become more significant and can make a real difference to people's lives. As such, various aspects of these systems need to be carefully investigated and analysed, including their security/privacy issues. In this paper, we present our work in designing and implementing various technological features that can be used to assist domestic violence survivors in obtaining help without leaving traces which might lead to further violence from their abuser. This case study serves as the core of our paper, in which we outline our approach, various design considerations – including difficulties in keeping browsing history private, our currently implemented solutions (single use URL, targeted history sanititation agent, and secret graphical gateway), as well as novel ideas for future work (including location-based service advertising and deployment in the wild).

Keywords: Privacy; confidentiality; practical security; browsing history; social inclusion; survivors; domestic violence; intimate partner cyber stalking; support groups; system implementation; work in progress.

1 Introduction

As more and more people are embracing online social networking applications, various concerns have been raised with regard to the security and privacy issues associated with such applications. There have been documented cases and reports regarding violations of user privacy by some of the big companies providing these services (e.g. [18] and [19]), although in most cases, their users seem to be rather oblivious to the threats of supplying their details online without much consideration. It is often stated that human players are usually the weakest link when it comes to computer security [4][9][12], so it is very important to provide a system that requires minimum effort from its users.

When it comes to the consequences of privacy violation, a very poignant example can be drawn from our experience in designing and implementing a system to assist survivors of domestic violence – the term "survivors" is used rather than "victims", as it more accurately describes the individuals who have lived with domestic abuse [17].

There are a number of published works which highlight the issues of domestic abuse and that there is a clear link with *intimate partner cyber stalking* [6][10][13][14]. There are two aspects to the issue: first, an intimate partner (ex or current) has a greater level of access to and knowledge about the habits of the survivor; second, the cyber stalking is a new and powerful weapon which adds to the ways in which the survivor can be controlled and/or coerced. These works also highlight that the survivors who are being stalked by their partner or ex-partners are of a greatly increased risk of being harmed [10], and that stalking behaviour (whether conducted in cyber space or not) could be viewed as a warning sign of an escalation towards violence. For example, evidence compiled by the US Department of Justice suggests that 81% of women who were stalked by partners were also assaulted by the same partner [16], while the Metropolitan Police found that 40% of domestic violence murders in London were also victims of stalking [11].

Previous studies [3][13] identify that telephones and mobile phones are the most commonly used technology in cases of cyber stalking. Statistics published by the US Department of Justice [3] also show that among 2.4 million victims of cyber stalking in the US, 30.3% of which were stalked by a current or ex-partner, which equates to around 730,000 cases of cyber stalking during 2008. Equally alarmingly, the same report also provides details of the high-tech methods used to monitor the activities of victims, including spyware, video and webcams, listening devices and GPS. In the UK, a survey carried out by the University of Bedfordshire [7] showed that 31.6% of stalkers were either ex-boyfriends (21.2%) or ex-partners (10.4%). Moreover, a report published by the Network for Surviving Stalking and Women's Aid Federation of England [10] details a number of different examples of women being stalked through Facebook, eBay, geotagging, and – most worrying of all – through applications previously loaded onto their smart phone by their abuser which tracks the victims location without their knowledge. However, digital technologies and electronic footprints can also be used to record the actions of abusers, the evidence of which can be used as evidence against them (although this is quite difficult) [15].

1.1 Problem Statement

As we go about our daily lives we are unwittingly leaving *electronic footprints*, which can easily be followed to see what we have been up to. This is because the technologies we use in our everyday lives (such as Internet browsers, mobile phones/smartphones, land lines, and GPS units) maintain records of our activities, which for most of us serve as a convenient aide-mémoire so that we do not have to remember "the number of someone who called yesterday", "the meeting time agreed in an SMS" or "the URL of the website I visited".

In addition to these passive data gathering features, there are also a number of incredibly useful monitoring applications aimed at keeping our children safe, which pro-actively make use of the data collected from Internet monitoring tools, such as *CheckStick* – `http://www.checkstick.com`, which tells you what your kids are looking at online. In most cases, these tools are very valuable to keep their users safe, but for survivors of domestic violence, these convenient features and monitoring tools

can become an instrument of abuse, in that it allows an abuser to track the survivor's activities even when the abuser is not present, and thereby control/restrict the activities of the survivor. For example, the abuser can control who the survivor can communicate with, monitor what the survivor looks at online, and trace where the survivor travels. All these lead to the intimate partner cyber stalking mentioned earlier.

The reality for a survivor is that any attempt to seek help, either from friends and family or from support organisations, is likely to attract attention and possibly further abuse. This has the effect that although technology is providing more convenient ways for survivors to access the help they require, it is also preventing survivors from accessing those resources. Current Internet browser and mobile phone technologies make it relatively easy for an abuser to review the electronic records that the survivors have collected; conversely it requires a much greater level of technical knowledge and quite a lot of work on the part of the survivors to cover their tracks.

Therefore the technologies that are designed for our convenience inadvertently put survivors at a technological disadvantage. One way to address this problem is by erasing survivor's electronic footprints, but this is not as straightforward as it sounds. Internet browsers and mobile phones will (by default) record their actions, but using a "clear all" approach leaves large gaps in the history, which can also raise abuser's suspicion. To make matters worse for the survivors, each technology stores data in a different way, requiring extra knowledge and effort to effectively remove the traces of their activities. In some cases, data such as mobile phones billing records cannot be altered by the user, leaving them with very limited or even no options.

Key Requirements. The proposed system aims to benefit survivors of domestic violence. These survivors tend to have limited knowledge and experience with technology, and in some cases, English is not their first language [17]. As such, the system needs to be *very easy to use*, with minimal interaction required with its users. In fact, being *invisible* is another key requirement, so that the system does not draw attention from the survivors' abuser. Most – if not all – of the technical activities (such as installing and configuring the proposed system) will be performed by staff at the support centre, with assistance from the authors/developers of the system.

Attacker Model. The main potential attackers will be the survivors' partner (and abuser). They have access to or control of the (shared) computer at home or even the survivors' smartphones. They have sufficient computer knowledge (for example, they know how to check web browser history), but they are not a hacker or an expert in computer security or forensic. They will not monitor the survivors' computer usage all the time (e.g. no key logger or network sniffer will be used). Nonetheless, it is expected that the attacker will be able to take control of the survivor's computer *after* the survivor finishes using it to access domestic violence support websites. Therefore one of the main aims of our proposed solutions (see Section 3) is to remove traces of digital footprints associated with domestic violence support websites from any devices used by the survivors.

1.2 Related Work in Privacy Enhancing Technologies

Issues related to private browsing are not new, and many papers have addressed them to various levels and from different perspectives. Aggarwal et al. [1], considers two types of attackers threatening private browsing: *local attacker* (family member or other people who has access to the user's machine and might be able to examine its browser's history) and *web attacker* (web sites trying to track and collect data from the user's visit).

Plenty of research has been done in dealing with web and third-party attackers (for example [2][8][20][22]). In our work, however, we are interested in defending against local attackers, which include survivors' abusers in the domestic violence scenario. Portable versions of the popular Internet browsers that allow private or incognito browsing (e.g. Google Chrome [21]) are available to defend against local attackers. There are even more comprehensive solutions such as Tails [23] (which can be deployed as a live USB stick or DVD for preserving anonymity), containing a set of online anonymity tools including Tor [24].

If used correctly, these solutions represent the most effective way of achieving privacy. But they rely on the user being technically savvy or even remembering to turn on and use these features. This is often not the case with survivors of domestic violence. Their knowledge of computer technologies, security and privacy is usually very limited, so it is unreasonable to expect them to be able to use complex features provided by these solutions. Moreover, it is not possible to use USB stick or CD/DVD when accessing information on a mobile phone. Therefore, these solutions – even though they are widely available and provide excellent features for private browsing – constitute only one of the layers of protection that we envisage will be necessary for achieving privacy for these survivors.

2 Case Study: Experience with Survivors

In this paper, we focus on a case study involving survivors who attend a women's support centre for Black and Minority Ethnic (BME), based in the UK (for privacy reasons, we do not state the name of this support centre, instead we refer to it as our "case study"). Data collection was performed using an online survey through several sessions organised by the support centre's staff, in which, groups of survivors as well as women from the control group completed the online survey.

This case study provides us with important insights and experience in the design and development of socio-technical systems where privacy is one of the key features. It also allows us to come up with novel ideas on how new technologies can be used for ensuring privacy. Some of these ideas are still to be implemented, but we are confident that they will contribute positively in improving users' privacy, while being usable and practical at the same time. We are also planning to carry out evaluation of the whole system once it is fully implemented.

The research shows that survivors have two major barriers to successfully accessing the support services that they require [17]:

- locating the support services and the organisations that provide them, and
- fear of provoking further abuse if their abuser discovers that they have been seeking help (hence their reluctance to report the incidents to the police or relatives).

In effect, survivors are being excluded from the socio-technical systems that the rest of us take for granted, largely because they are afraid of using these systems for fear of being found out looking for help. This paper proposes a digital strategy for the social inclusion of survivors. The strategy incorporates several technology-based solutions and a training strategy, which together will help to overcome these barriers. The aims are to publicise domestic violence support services in a way that is most accessible to survivors, while at the same time providing technological solutions that help survivors avoid leaving telltale electronic footprints.

2.1 Method and Implementation

The overall aim of this case study is the *social inclusion of survivors through technology*, and to achieve this, the tasks have been divided into a number of sub-goals:

- Understand how survivors currently relate to technologies that would be useful to them and the technological issues that they face
- Propose a digital strategy to make domestic violence support services more accessible
- Propose a range of technological solutions that help survivors avoid leaving telltale electronic footprints

In order to address these goals, we have worked closely with the staff at the case study's support centre to understand the technological issues faced by survivors. The guidance given by the case study's staff has been invaluable in the development of the technology strategy.

Due to the sensitive nature of the subject, it was not appropriate to use standard user interview techniques to gather the data required. It was felt that an online survey would be a less intrusive way to gather the data, as this could be carried out in the familiar surroundings of the case study's facility with the assistance of its staff, without requiring a member of our research team to be present. The women who completed the survey were selected from women regularly attending services provided by the centre. There were two groups of these women: survivors of domestic violence, and a control group of women who attend the centre for other activities (not related to domestic violence, such as learning English language or new skills). The data were collected from the control group to minimise the influence of other factors common to all women attending this centre, such as socio-economic and/or ethnic group.

The survey collected information relating to the following topics: (i) the location of the computer the women used to access the internet; (ii) websites visited, including any online support services used; (iii) other communications channels such as instant messaging; (iv) type and capabilities of mobile phones used; (v) indication of age range (to eliminate any age related trends); (vi) whether survivors felt they were being monitored; (vii) which support services survivors would like to see implemented.

Two online survey forms were used to collect the data, one for survivors and one for the control group. The control group were not asked questions specifically relating to domestic violence. A multiple-choice format was utilised to obtain the granularity required and ensure the uniformity of terminology used in responses. The forms can be viewed at:

`http://research.cs.ncl.ac.uk/surveys/survivors-survey.html` and `http://research.cs.ncl.ac.uk/surveys/womens-survey.html`.

There are two competing considerations when deciding which support services would best serve the needs of the survivors:

- preference of the survivors – there is no point providing services which survivors do not want or will not use
- affordability/running costs – it would be counter-productive to create a support service for survivors which has to be withdrawn because it is too expensive to run

Our choices regarding which technologies to use are therefore influenced by these factors and we also endeavour to develop a system that is as easy to use as possible.

2.2 Lessons Learnt

Our contact with the case study commenced in June 2010, and it has involved close collaboration with the staff at the support centre. From this collaboration, we have been able to draw insights and initial conclusions about the issues faced by survivors and the support services used by survivors [17].

One of the major challenges that survivors face is that it requires more effort and more technical knowledge for them to erase their *electronic footprints*, than it does for their abuser to follow them. It is interesting to notice that survivors seem to be aware of the feature of Internet browsers to record the history of the pages they have visited, and that survivors are keen to be able to avoid this. Therefore redressing the balance in favour of the survivor will require a range of measures including redesigned web-sites, history cleaning technologies and training.

Table 1. Technologies usage of survivors.

Category	Survivors	Control
Access to the Internet	71%	100%
Access to computer outside the home (friends, relatives, library)	29%	87%
Used Internet communications such as Skype and IM	43%	87%
Mobile phone usage / ownership	86%	87%

A survey of survivors was performed as part of the case study, to capture first-hand their opinions. A total of 22 women completed the online survey, the results of which have provided valuable insights into – among others – the technology usage of survivors. **Table 1** provides a summary of the survivors' usage of technology as compared to that of the control group. The survey results show that the survivors in our sample are 29% less likely than others in their socio-economic/cultural/ethnic group to be

regularly using the Internet and the support services it provides. Encouragingly, the survey also shows that mobile phone usage amongst survivors is pretty much equal to that of the control group of the sample. Although survivors did not express a strong preference for an Internet browser that does not record history, it is felt from our reading of related works mentioned in Section 1 that this will be a valuable tool to implement for survivors. Further information regarding the survey can be found in [17].

3 Proposed Solutions

Our research proposes a number of technology solutions to improve survivors' access to domestic violence support services. We are also focusing on providing a feature for erasing survivors' digital footprints without raising suspicion to their abusers.

3.1 More Accessible Domestic Violence Support Services

There are technologies that can improve the accessibility of support services by ensuring that survivors are not excluded because they do not know that the support service is there. These include *Quick Response* (QR) codes, as well as *Near Field Communication* (NFC) and *Radio Frequency Identification* (RFID) tags.

Fig. 1. QR code example containing a single use URL.

QR codes are printed two-dimensional barcodes (**Fig. 1**) that can encode a URL or a SMS text message and can be read by a smartphone or a laptop with a webcam, allowing easy dissemination of web pages. NFC and RFID tags are a class of wireless information storage device that can store much more data than a QR code and can be read by some smartphones and computers.

With smartphones capable of reading QR codes – and even NFC and RFID tags – becoming more accessible and readily available for survivors to use, we propose embedding information in real world objects using these technologies.

Imagine that you are a close friend or family member of a survivor who is still in an abusive relationship and you want to help by letting her know about online support services which can help, without alerting her partner. What is required is a way of hiding the URL in an everyday object that will not arouse suspicion. QR codes can be printed on self-adhesive labels, making it easy to attach a URL to any real-world ob-

ject; this could be a poster or flyer advertising the support service or other everyday objects such as a postcard from a friend or on the base of a mug thereby disguising its meaning.

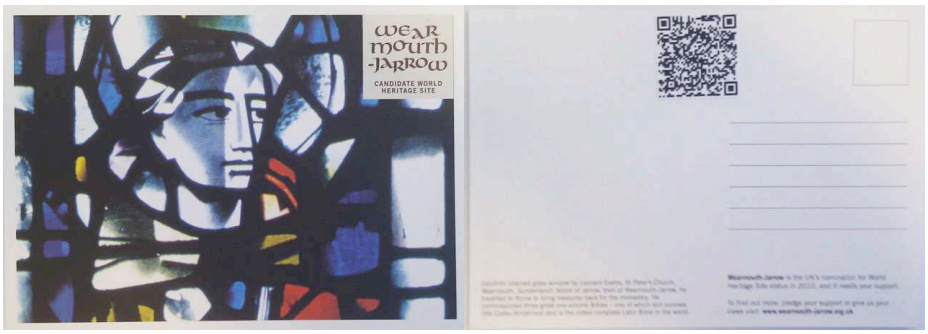

Fig. 2. Postcard with QR code – front (left) and back (right).

An example of a QR code embedded in an innocent-looking postcard can be seen in **Fig. 2**. The QR code in **Fig. 1** can be read with a smartphone and contains a URL which points to a live demo of "single use URL access codes" (see Section 3.2).

QR codes are very cost effective because free software applications can be used to print them, so the only costs are the printing and the sticky labels. This compares very favourably with the cost of NFC, currently around £1.50 per item. NFC tags are much more expensive than QR codes so their use would be limited to applications where the additional functionality they provide is worth the extra expense. NFC objects can carry a great deal more information than QR codes, this provides the opportunity to embed more data. For example, an NFC tag could be used to store a list of all support services in the local area. These tags could then be attached to posters advertising support services, and the survivors can download and view the whole list on their phone without having to connect to the Internet. NFC tags can also give a unique response to each person who accesses the information; this would allow posters to be created that will hand out a different single use URL to each smartphone that accesses the poster.

3.2 Erasing the Digital Footprints of Survivors

Allowing survivors to freely access online resources whilst hiding their activities from their abusers is a complex problem that does not have a single solution. Our approach consists of a number of complementary technologies that provide layers of protection.

Single Use URL Access Codes. Given that a survivor may forget (or even not be aware of how) to use the private browsing feature, or do not know how to clear their history after accessing domestic violence support services online, it is proposed that specific sections of domestic violence websites could incorporate an automatic means of sanititising the browser history of anyone who visits the website.

Our solution hides pages relating to domestic violence support services behind "innocent pages" from a real website that the survivor would quite legitimately use. The website is designed with both innocent pages and domestic violence pages, anyone entering the website without a valid access key would be given innocent pages only.

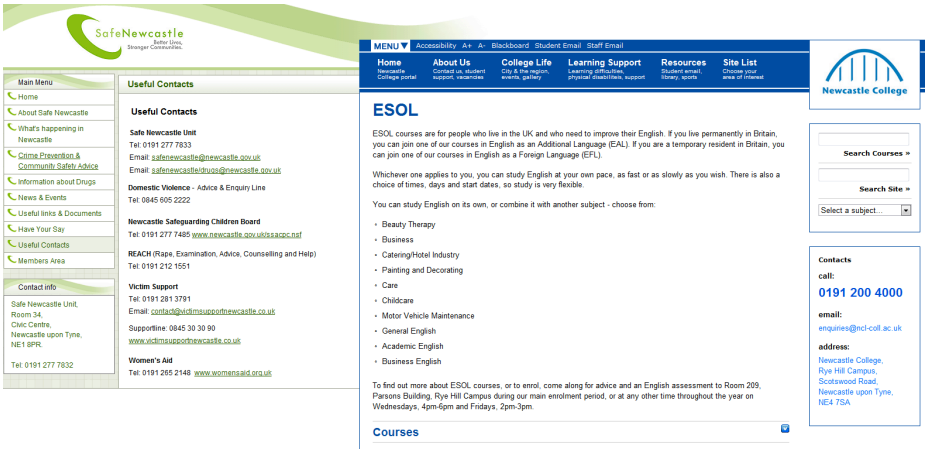

Fig. 3. Domestic violence support directory page (left) and innocent replacement page (right).

This example uses content for ESOL (English for Speakers of Other Languages) courses as the innocent pages, this matches the profile of the women who use the case study's services, many of whom attend ESOL courses to improve their English. Different centres will use different innocent pages, to match the profile of the women attending the different centres. Each access key may only be used *once*; all subsequent attempts to access the domestic violence pages with a used access key will result in innocent pages being presented (an example can be seen in **Fig. 3**). This stops the abuser from following the browser history to the domestic violence support pages.

The access codes can be distributed in various ways; the method selected should draw the least attention for the survivors who will be using them. Some of the methods we envisage using include: embedding QR codes on postcards, posters, flyers or objects, providing a USB stick containing tools that survivors can use, emailing the URL to survivors, printing the URL on tear-off strips at the bottom of a poster, and sending the URL as a text message.

An algorithm will generate access codes based on the date, so that codes will be valid for a limited time. The access code algorithm will incorporate a checksum to stop random numbers being accepted as valid access codes.

We have implemented a prototype of this solution.

Location-based Service Advertising. A poster advertising a particular domestic violence support service will be placed in a public location (e.g. bus stops, shopping malls, local shop windows or in the window of the service provider). The poster allows survivors to access online domestic violence service pages and resources on their mobile phone whilst they are at the location of the poster, however once they

leave the location, the URL cannot be accessed using the history or back button. This feature will be facilitated by the single use URL mechanism (described previously), which provides the domestic violence support service the first time the URL is used; any subsequent request using the URL code will result in an innocent page being displayed.

Unlike the static Quick Response (QR) codes on postcards/sweets, the poster will give a new single use URL each time a user passes their phone close to the poster. A programmable Near Field Communication (NFC) smart tag is capable of running a small JavaCard program, which will produce a new unique URL for each request. The JavaCard program uses an algorithm to calculate the single use URLs, each URL will be unique and will conform to the validation routine on the web site providing the domestic violence support service.

We will implement this solution soon.

Targeted History Sanitisation Agent. The objective of history sanititation agent is to automatically erase the digital footprints left behind when a user accesses specific support websites, by removing all history entries related to the support websites, including temporary Internet files, browser history entries, and cookies.

The agent will leave intact all other history entries, thereby avoiding making it look like the PC has been cleaned. The agent will automatically download a list of support websites, which will be used to decide which entries to delete; the list will be updated by support centre staff when new support websites go online.

Smartphones are becoming an increasingly popular way for accessing online content. We are therefore developing versions of the history sanitisation agent for Android and iPhone platforms as well. The smartphone agent development has also investigated the ability to automatically cleanse the phone of unwanted entries in the call and SMS history lists. Installation of this agent on smartphones will be carried out at the support centre. It is a bit trickier to deploy the targeted history sanititation agent on the survivors' computer, which tend to be a shared PC at home that their abuser also has access to. We envisage packaging the agent – along with portable anonymous browsers and other privacy tools – into a USB stick or a live CD/DVD that can be distributed to survivors. Training on how to use these tools will be given to survivors by staff at the support centre.

We have implemented a prototype of this solution for Microsoft Windows based PCs supporting various web browsers, as well as for Android smartphones.

Secret Graphical Gateway. The idea is to design and implement an application that will display a set of pictures as the front end of the gateway. When a survivor clicks the correct number of points in the right coordinates on the right picture and in the right sequence (set-up beforehand), the application will direct them to the support services site, otherwise it will do nothing. This way, the application will look innocent and will not raise suspicion to the survivor's abuser. In fact, this gateway application could be disguised as a digital picture viewer. In a sense, this is comparable to graphi-

cal password (e.g. [5]), albeit being "invisible" in its nature (without any signposting or obvious interactive feature that might attract attention).

We have implemented a prototype for Android smartphones.

4 Conclusion and Future Work

Through this work, we have demonstrated the need for solutions that will have a significant impact on social inclusion for survivors of domestic violence by improving the accessibility of domestic violence support service and by improving the ability of survivors to avoid leaving electronic footprints when they access these services. The case study shows that existing technologies utilised by survivors unintentionally work contrary to these aims. Given that this situation is unlikely to change and there is a limited budget for this project, we have adopted a strategy that proposes a set of bite-sized solutions, each of which will be relatively quick implement at a modest cost.

We have implemented and tested the single use URL access codes idea, the targeted history sanititation agent, as well as the secret graphical gateway. However, wider deployment and further evaluation of the effectiveness of these solutions are still to be carried out. We will complete the implementation of other novel ideas, including the location-based domestic violence support advertising proposed in Section 3.2, either as proof of concept demonstrations or as fully functional solutions soon.

We plan to continue working with the case study's staff and survivors, to gather additional data and results through questionnaires and "in the wild" deployment of the proposed solutions, including their usability assessment. We will also explore other potential avenues for effective solution by conducting participatory, experience-centred design process with the survivors and the staff at the support centre.

Acknowledgement

We would like to thank the staff at the support centre of the case study, as well as the survivors who participated in our survey for providing invaluable insights into the survivors' story. We also appreciate the anonymous reviewers' feedback and comments, which helped us improve this paper.

References

1. Aggrawal, G., Bursztein, E., Jackson, C., Boneh, D.: An analysis of private browsing modes in modern browsers. In: Proceedings 19th USENIX Security Symposium (2010)
2. Krishnamurthy, B., Malandrino, D., Wills, C.E.: Measuring privacy loss and the impact of privacy protection in web browsing. In: Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07), ACM, New York, NY, USA, 52–63 (2007)
3. Baum, K., Catalano, S., Rand, M., Rose, K.: Stalking victimization in the US. US Department of Justice National Crime Victimisation Survey, January (2009)
4. Besnard, D., Arief, B.: Computer security impaired by legitimate users. Computers & Security, 23(3), 253–264, May (2004)

5. Dunphy, P., Yan, J.: Do background images improve "draw a secret" graphical passwords? In: Proceedings of the 14th ACM conference on Computer and Communications Security (CCS '07), ACM, New York, NY, USA, 36–47 (2007)
6. Logan, T., Walker, R.: Partner stalking: Psychological dominance or business as usual? Trauma Violence Abuse, 10(3), 247–270, July (2009)
7. Maple, C., Short, E., Brown, A.: Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey. University of Bedfordshire National Centre for Cyberstalking Research (2011)
8. Mayer, J.R., Mitchell, J.C.: Third-Party Web Tracking: Policy and Technology. In: Proceedings of the IEEE Symposium on Security and Privacy, 413–427 (2012)
9. Mitnick, K., Simon, W.: The art of deception: Controlling the human element of security. Wiley (2002)
10. Perry, J.: Digital stalking: A guide to technology risks for victims. Published jointly by Network for Surviving Stalking and Women's Aid Federation of England (2012)
11. Richards, L.: Findings from the Multi-agency Domestic Violence Murder Reviews in London. Prepared for the ACPO Homicide Working Group, Metropolitan Police (2003)
12. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the weakest link - a human computer interaction approach to usable effective security. BT Tech. Journal, 19, 122–131 (2001)
13. Southworth, C., Dawson, S., Fraser, C., Tucker, S.: A high-tech twist on abuse: Technology, intimate partner stalking and advocacy. Violence Against Women Online Resources. June (2005)
14. Southworth, C., Finn, J., Dawson, S., Fraser, C., Tucker, S.: Intimate Partner Violence, Technology, and Stalking. Violence Against Women, 13(8), 842–856, (2007)
15. Spence-Diehl, E.: Stalking and technology: The double edge sword. Technology in Human Services, 22(1), 5–18 (2003)
16. Tjaden, P., Thoennes, N.: Stalking in America: Findings form the national violence against women survey. US Dept. of Justice (1998)
17. van Moorsel, A., Emms, M., Rendall, G., Arief, B.: Digital Strategy for the Social Inclusion of Survivors of Domestic Violence. Technical Report CS-TR-1277, School of Computing Science, Newcastle University, September (2011)
18. BBC News Online: Details of 100m Facebook users collected and published, http://www.bbc.co.uk/news/technology-10796584, last accessed: 27 November 2012
19. BBC News Online: Facebook's battle with privacy and profit. http://news.bbc.co.uk/1/hi/programmes/click_online/8843007.stm, last accessed: 27 November 2012
20. Digital Trends: Why Do Not Track may not protect anybody's privacy. http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy/, last accessed: 27 November 2012
21. Google Chrome: Using the Incognito mode. https://support.google.com/chrome/bin/answer.py?hl=en-GB&answer=95464&p=cpn_incognito, last accessed: 27 November 2012
22. Panopticlick: How Unique – and Trackable – Is Your Browser? https://panopticlick.eff.org/, last accessed: 27 November 2012
23. Tails: The Amnesic Incognito Life System. https://tails.boum.org/, last accessed: 27 November 2012
24. Tor Project: Anonymity Online. https://www.torproject.org/, last accessed: 27 November 2012